AFRL-OSR-VA-TR-2015-0173

CONGRESSIONAL) CYBERSECURITY OF CRITICAL CONTROL NETWORKS

William Mahoney
UNIVERSITY OF NEBRASKA

07/14/2015
Final Report

Air Force Research Laboratory
AF Office Of Scientific Research (AFOSR)/ RTC
Arlington, Virginia 22203
Air Force Materiel Command

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
07-07-2015	Final	07/01/2010-06/30/2015

4. TITLE AND SUBTITLE
(Congressional) Cybersecurity of Critical Control Networks

5a. CONTRACT NUMBER

5b. GRANT NUMBER
FA9550-10-1-0341

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Dr. William Mahoney

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
University of Nebraska, University of Nebraska at Omaha, 6001 Dodge Street, EAB 209, Omaha, Nebraska 68182-2000

8. PERFORMING ORGANIZATION REPORT NUMBER
45-0806-1010-100

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
AFOSR/PKR1, USAF, AFRL
AF Office of Scientific Research
875 N. Randolph St. Room 3112
Arlington, VA 22203

10. SPONSOR/MONITOR'S ACRONYM(S)
AFOSR/PKR1

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Publicly available/unclassified

13. SUPPLEMENTARY NOTES
Final Report

14. ABSTRACT

We have funded several research projects that have yielded a large number of publications and conference presentations in the area of Supervisory Control And Data Acquisition (SCADA). Details of each project are included below. The tasks include work in link encryption for existing legacy SCADA equipment, where we continue to develop lightweight encryption schemes applicable for low bandwidth low energy environments such as the smart grid. We have investigated the use of a domain specific language for authoring and monitoring compliance of SCADA systems, including technologies for a "policy monitor" which reports out on any observance issues. We worked with students in the Computer Engineering School at the University of Nebraska Lincoln to design and implement a low-cost hardware-in-the-loop device, which can be used to mimic the activities in an industrial control system. Specific to the transportation industry, we participated in an investigation of SCADA systems in airports, which we reported on at a conference and also a journal paper. We have conducted extensive investigations into the hardware purchased under this AFOSR award from Allen-Bradley and Rockwell Automation. These investigations have yielded several important technical publications.

15. SUBJECT TERMS
SCADA; critical infrastructure; standards compliance; reverse engineering

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. William Mahoney
U	U	U	UU	6	19b. TELEPHONE NUMBER *(Include area code)* 402-554-3975

Reset

INSTRUCTIONS FOR COMPLETING SF 298

1. REPORT DATE. Full publication date, including day, month, if available. Must cite at least the year and be Year 2000 compliant, e.g. 30-06-1998; xx-06-1998; xx-xx-1998.

2. REPORT TYPE. State the type of report, such as final, technical, interim, memorandum, master's thesis, progress, quarterly, research, special, group study, etc.

3. DATES COVERED. Indicate the time during which the work was performed and the report was written, e.g., Jun 1997 - Jun 1998; 1-10 Jun 1996; May - Nov 1998; Nov 1998.

4. TITLE. Enter title and subtitle with volume number and part number, if applicable. On classified documents, enter the title classification in parentheses.

5a. CONTRACT NUMBER. Enter all contract numbers as they appear in the report, e.g. F33615-86-C-5169.

5b. GRANT NUMBER. Enter all grant numbers as they appear in the report, e.g. AFOSR-82-1234.

5c. PROGRAM ELEMENT NUMBER. Enter all program element numbers as they appear in the report, e.g. 61101A.

5d. PROJECT NUMBER. Enter all project numbers as they appear in the report, e.g. 1F665702D1257; ILIR.

5e. TASK NUMBER. Enter all task numbers as they appear in the report, e.g. 05; RF0330201; T4112.

5f. WORK UNIT NUMBER. Enter all work unit numbers as they appear in the report, e.g. 001; AFAPL30480105.

6. AUTHOR(S). Enter name(s) of person(s) responsible for writing the report, performing the research, or credited with the content of the report. The form of entry is the last name, first name, middle initial, and additional qualifiers separated by commas, e.g. Smith, Richard, J, Jr.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES). Self-explanatory.

8. PERFORMING ORGANIZATION REPORT NUMBER. Enter all unique alphanumeric report numbers assigned by the performing organization, e.g. BRL-1234; AFWL-TR-85-4017-Vol-21-PT-2.

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES). Enter the name and address of the organization(s) financially responsible for and monitoring the work.

10. SPONSOR/MONITOR'S ACRONYM(S). Enter, if available, e.g. BRL, ARDEC, NADC.

11. SPONSOR/MONITOR'S REPORT NUMBER(S). Enter report number as assigned by the sponsoring/ monitoring agency, if available, e.g. BRL-TR-829; -215.

12. DISTRIBUTION/AVAILABILITY STATEMENT. Use agency-mandated availability statements to indicate the public availability or distribution limitations of the report. If additional limitations/ restrictions or special markings are indicated, follow agency authorization procedures, e.g. RD/FRD, PROPIN, ITAR, etc. Include copyright information.

13. SUPPLEMENTARY NOTES. Enter information not included elsewhere such as: prepared in cooperation with; translation of; report supersedes; old edition number, etc.

14. ABSTRACT. A brief (approximately 200 words) factual summary of the most significant information.

15. SUBJECT TERMS. Key words or phrases identifying major concepts in the report.

16. SECURITY CLASSIFICATION. Enter security classification in accordance with security classification regulations, e.g. U, C, S, etc. If this form contains classified information, stamp classification level on the top and bottom of this page.

17. LIMITATION OF ABSTRACT. This block must be completed to assign a distribution limitation to the abstract. Enter UU (Unclassified Unlimited) or SAR (Same as Report). An entry in this block is necessary if the abstract is to be limited.

Report for the Nebraska University Consortium on Information Assurance
July 1, 2010 – June 30, 2015
For US Department of Defense/Air Force Office of Scientific Research
In Regards to FA9550-10-1-0341 Cybersecurity of Critical Control Networks

Report Type
Final Report

Primary Contact E-mail
wmahoney@unomaha.edu

Primary Contact Phone Number
402-554-3975

Organization / Institution name
University of Nebraska at Omaha

Award Information

Grant/Contract Title
Cybersecurity of Critical Control Networks

Grant/Contract Number
FA9550-10-1-0341

Principal Investigator Name
Dr. William Mahoney

Program Manager
The AFOSR Program Manager currently assigned to the award
Dr. Tristan Nguyen

Report Information - Final Report

Reporting Period Start Date
July 1, 2010

Reporting Period End Date
June 30, 2015

Report Abstract:

Abstract: Under AFOSR award number FA9550-10-1-0341, we have funded several research projects that have yielded a large number of publications and conference presentations in the area of Supervisory Control And Data Acquisition (SCADA). Details of each project are included below. The tasks include work in link encryption for existing legacy SCADA equipment, where we continue to develop lightweight encryption schemes applicable for low bandwidth low energy environments such as the smart grid. We have investigated the use of a domain specific language for authoring and monitoring compliance of SCADA systems, including technologies for a “policy monitor” which reports out on any observance issues. We worked with students in the Computer Engineering School at the University of Nebraska Lincoln to design and implement a low-cost hardware-in-the-loop device, which can be used to mimic the activities in an industrial control system. Specific to the transportation industry, we participated in an investigation of SCADA systems in airports, which we reported on at a conference and also a journal paper.

We have conducted extensive investigations into the hardware purchased under this AFOSR award from Allen-Bradley and Rockwell Automation. These investigations have yielded several important technical publications as well as more recently an event we reported to ICS-CERT and to Rockwell. We used a method called “learned event patterns” to work on a simple system for intrusion detection or anomaly detection within SCADA systems. All of these research projects have yielded publications and have advanced the state of the art in SCADA research, as well as funding important undergraduate and graduate student experiences.

Upload a Report Document, if any. The maximum file size for the Report Document is 50MB.

Additional Information

Archival Publications (published) during reporting period:

Authentication Bypass and Remote Escalated I/O Command Attacks, Ryan Grandgenett, William Mahoney, Robin Gandhi, 10th Cyber and Information Security Research Conference, Oak Ridge, Tennessee, April 2015.

Hardware Implementation of Quasigroup Encryption for SCADA Networks, William Mahoney, Abhishek Parakh and Matthew Battey, The 13th IEEE International Symposium on Network Computing and Applications (IEEE NCA14), August 2014, Cambridge, MA.

Exploitation of Allen Bradley’s Implementation of EtherNet/IP for Denial of Service Against Industrial Control Systems, Ryan Grandgenett, Robin Gandhi and William Mahoney, 9th International Conference on Cyber Warfare and Security, Purdue University, March 2014.

My PLC Makes an Excellent Web Server, William Mahoney, 9th International Conference on Cyber Warfare and Security, Purdue University, March 2014.

SCADA Threats in the Modern Airport; John McCarthy, William Mahoney, International Conference on Information Warfare, Denver CO, March 2013.

SCADA Threats in the Modern Airport; John McCarthy, William Mahoney, International Journal of Cyber Warfare and Terrorism, Vol. 3 No. 4, pp 32-39, October-December 2013. (A revision of the above paper, requested by the journal.)

Smart Grid Tamper Detection using Learned Event Patterns; (book chapter) William L. Sousan, Quiming Zhu, Robin Gandhi, and William Mahoney, to appear in “Systems and Optimization Aspects of Smart Grid Challenges”, Optimization and Security Challenges in Smart Power Grid, Springer, pp 99-115. (http://link.springer.com/book/10.1007%2F978-3-642-38134-8)

Optimal Values for Disrupting x86-64 Reverse Assemblers, Sara Shinn, William Mahoney, International Journal of Computer Science and Network Security, Volume 11, Number 11, November 2011.

Using Anomalous Event Patterns in Control Systems for Tamper Detection, William Sousan, Robin Gandhi, Qiuming Zhu, William Mahoney, CSIIRW-7 Cyber Security and Information Intelligence Research Workshop, Oct 12-14, 2011, Oak Ridge, Tennessee.

Towards a Low-Cost SCADA Test Bed: An Open-Source Platform for Hardware-in-the-Loop Simulation, The 2011 International Conference on Security and Management, Special Track on Mission Assurance and Critical Infrastructure Protection (STMACIP’11), Las Vegas, Nevada, Nicholas Wertzberger, Casey Glatter, William Mahoney, Robin Gandhi, Kenneth Dick.

An Integrated Framework for Control System Simulation and Regulatory Compliance Monitoring, International Journal of Critical Infrastructure Protection (IJCIP), Vol. 4, 2011. Mahoney, W., Gandhi, R.A.

Language-driven Assurance for Regulatory Compliance of Control Systems; Proceedings of the 5th International Conference on Information Warfare and Security, April, 2010, authors Robin Gandhi, William Mahoney, Ken Dick, Zachary Wilson.

ADACS – A Language for Monitoring Regulatory Compliance in Control Systems; Second Workshop on Compiler and Architectural Techniques for Application Reliability and Security, the 39th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, Estoril, Portugal, authors Robin Gandhi, William Mahoney, Ken Dick.

Cryptanalysis and Improvements of the Quasigroup Block Cipher: Journal of Information Assurance and Security (JIAS), Volume 10 Issue 1, January 2015, pp 31-39, authors Matthew Battey, Abhishek Parakh and William Mahoney.

Data Acquisition and Processing of Sensor Data in a General Body Area Network, the Biomedical Science and Engineering Conference - Collaborative Biomedical Innovations, Oak Ridge, USA, May 6, 2014. Austin Shores, Chee Vang, Yaoqing Yang.

A poster presentation was made at the 2013 Council on Undergraduate Research Conference of Research Experiences for Undergraduates Student Scholarship (CUR CREUSS) in Arlington, VA.

A poster presentation was made at the 12th Annual Nebraska INBRE/BRIN meeting held in Grand Island, Nebraska, August 2013.

UNO students presented at the 2014 International Conference on Cyber Warfare and Security conference.

Modifications to GCC for Increased Software Privacy, William Mahoney, International Journal of Information and Computer Security. Accepted and awaiting publication.

Semantic Relevance Analysis of Subject-Predicate-Object (SPO) Triples, submitted to International Journal on Software and Knowledge Engineering, authors Ranjana Kumar, Robin Gandhi, William Mahoney, Parvathi Chundi, and Quiming Zhu.

Visual Analytics for Software Weaknesses, Tahmasbi, N., Gandhi, R., Siy, H., Submitted for conference publication

Changes in research objectives (if any): None

Change in AFOSR Program Manager, if any: Former Program Manager: Dr. Robert Herklotz

Extensions granted or milestones slipped, if any: None

Include any new discoveries, inventions, or patent disclosures during this reporting period (if none, report none):

We continue to utilize the funding for four concurrent research projects, which are detailed below.

- **Exploration of Language-Driven Compliance:** We created a novel approach to precisely specify constraints mandated by regulatory requirements on a control system and implemented software to monitor the corresponding compliance status in near-real-time. Our research focused on the design of a language that bridges the gap between abstract regulatory policies and the realities of implementation.

Essentially, each regulatory check, a "policy monitor", is authored in a new language we are developing called ADACS (Autonomous component-based policy Description Language for Anomaly monitoring in Control Systems). The semantics of our language are closer to discrete real-time system interactions expressed as events encoded in XML messages, and the language is compiled into binaries of a general-purpose language that is portable across many hardware and software platforms.

Accomplishments: We presented the research at two conferences and one publication, and used this as a starting point on a SBIR grant which was subsequently awarded (Phase 1 only). This SBIR also yielded a chapter in a book on smart power grids.

- **Creation of a Low-Cost Hardware-in-the-loop Device:** We utilized funding through AFOSR in the creation of two devices used in our labs. First was a primitive PLC-like device, which could be programmed to toggle various I/O lines through a simple program. This was used to feed "live" data into the remainder of our lab infrastructure, providing a hardware-in-the-loop capability for simulations. A follow on project made a second unit that had a much simpler interface and could be commanded over a plain USB connection. Thus we can have a software simulation that drives actual hardware signals into the control equipment.

  Accomplishments: We reported out on the first of these two devices in a paper delivered at a Special Track on Mission Assurance and Critical Infrastructure Protection.

- **Improvements in Quasigroup Encryption for SCADA:** We have been working on link encryption schemes in the critical infrastructure protection realm with the intent of providing a low-cost low-overhead link encryption processor implemented in hardware. We've developed a preliminary version of the encryption system that's been published at various venues. We are constantly improving its strength against various cryptanalytic attacks and modifying its structure to better suite low-cost FPGA implementation.

  Accomplishments: This work is ongoing – now with more limited resources – but with promising results. We have reported on some of these results and are in the process of implementing newer versions of our work in smaller platforms to test the feasibility.

- **Reverse engineering of the CIP and EtherNet/IP protocols:** This project was one of the heavily emphasized areas explored with the funding from the award. The aim was to reverse engineer the EtherNet/IP protocol (this is Industrial Protocol and not Internet Protocol) and Common Industrial Protocol (CIP) standards and explore potential vulnerabilities. Two students were partially funded from a National Science Foundation summer research grant, while two faculty members were funded through AFOSR for research support. The aim of the work was to explore potential exploits and demonstrate the fragility of some Critical Infrastructure equipment.

  Accomplishments: We have exposed weaknesses in the Common Industrial Protocol (CIP) application data that can be carried over several different interfaces. We created a systematic process for reverse engineering of CIP messages from packet captures of a SCADA network and exposed vulnerabilities in this implementation of CIP for SCADA.Several papers have been published on our results (detailed in publications section). One flaw was sufficiently significant that the student and faculty submitted the results to ICS-CERT and then worked with Rockwell Automation to address the issue. For this work we utilize a test-bed environment that serves as a scale model of a real world oil pipeline. Reverse engineering of EtherNet/IP packets from the network traffic allowed us to determine the structure, command options, and potential vulnerable fields. Two students partially funded through AFOSR developed sophisticated Python programs to aid in the reverse engineering of captured CIP network traffic, and these tools have been shared with the industrial control researchers at Sandia National Labs. Our follow-on work will be to (A) expand our critical infrastructure equipment to include manufacturers suggested by external partners and to (B) create a CIP "fuzzer" to further investigate weaknesses within this protocol and associated equipment. This system will offer significant benefits to our national and economic security by protecting the integrity and availability of

pervasive automated communication processes between components on distributed insecure systems of vital infrastructure.

- **Exploration of Spoofing for Small PLCs:** For this project we explored the file system in a small Allen-Bradley PLC and determined whether it could be replaced with other code in order to fool the equipment operator into seeing false information.

  Accomplishments: We were able to download false HTML web pages into the device and give the illusion that the system was performing normally; we reported on these results at an international cybersecurity conference in Purdue.

- **Analysis of SCADA specific to Transportation:** An additional exploration area was the use of critical infrastructure protection relative to airport security. In conjunction with a European company in the airport security domain we examined specific equipment in an international airport and interviewed the IT staff.

  Accomplishments: We were surprised to discover that relative to other critical infrastructure domains, the airport domain is relatively secure as far as SCADA is concerned. Interestingly this is mainly due to the lack of SCADA equipment in critical areas rather than any particular vulnerabilities. We did report out on these findings at a conference that was reprinted as a journal article.

Partially sponsored by this research funding:

Dr. Bill Mahoney – Associate Professor, Information Assurance
Dr. Robin Gandhi – Associate Professor, Information Assurance
Dr. Ken Dick – Senior Research Fellow, IT Innovation
Mr. Charles Spence – Student Lab Manager
Ryan Grandgenett – Graduate student
Casey Glatter – Graduate student
Zachary Wilson – Graduate student
Nicholas Wertzberger – Undergraduate student
Michael Capito – Undergraduate student
Jon Grindstaff – Undergraduate student
Nithya Vangala – Graduate student
Victor Leading Horse – Undergraduate student
Rebecca Pray – Staff

Associated with the research efforts:

Dr. Abhishek Parakh – Assistant Professor, Information Assurance
Dr. William L. Sousan – PhD Graduate Student
Dr. Quiming Zhu – Professor, Computer Science

1.

1. Report Type

Final Report

Primary Contact E-mail

Contact email if there is a problem with the report.

wmahoney@unomaha.edu

Primary Contact Phone Number

Contact phone number if there is a problem with the report

402-554-3975

Organization / Institution name

University of Nebraska at Omaha

Grant/Contract Title

The full title of the funded effort.

(Congressional) Cybersecurity of Critical Control Networks

Grant/Contract Number

AFOSR assigned control number. It must begin with "FA9550" or "F49620" or "FA2386".

FA9550-10-1-0341

Principal Investigator Name

The full name of the principal investigator on the grant or contract.

Dr. William Mahoney

Program Manager

The AFOSR Program Manager currently assigned to the award

Dr. Tristan Nguyen

Reporting Period Start Date

07/01/2010

Reporting Period End Date

06/30/2015

Abstract

Under AFOSR award number FA9550-10-1-0341, we have funded several research projects that have yielded a large number of publications and conference presentations in the area of Supervisory Control And Data Acquisition (SCADA). Details of each project are included below. The tasks include work in link encryption for existing legacy SCADA equipment, where we continue to develop lightweight encryption schemes applicable for low bandwidth low energy environments such as the smart grid. We have investigated the use of a domain specific language for authoring and monitoring compliance of SCADA systems, including technologies for a “policy monitor” which reports out on any observance issues. We worked with students in the Computer Engineering School at the University of Nebraska Lincoln to design and implement a low-cost hardware-in-the-loop device, which can be used to mimic the activities in an industrial control system. Specific to the transportation industry, we participated in an investigation of SCADA systems in airports, which we reported on at a conference and also a journal paper. We have conducted extensive investigations into the hardware purchased under this AFOSR award from Allen-Bradley and Rockwell Automation. These investigations have yielded several important technical publications as well as more recently an event we reported to ICS-CERT and to Rockwell. We used a method called “learned event patterns” to work on a simple system for intrusion detection or anomaly detection within SCADA systems. All of these research projects have yielded publications and have

advanced the state of the art in SCADA research, as well as funding important undergraduate and graduate student experiences.

Distribution Statement

This is block 12 on the SF298 form.

Distribution A - Approved for Public Release

Explanation for Distribution Statement

If this is not approved for public release, please provide a short explanation. E.g., contains proprietary information.

SF298 Form

Please attach your SF298 form. A blank SF298 can be found here. Please do not password protect or secure the PDF
The maximum file size for an SF298 is 50MB.

AFD-070820-035.pdf

Upload the Report Document. File must be a PDF. Please do not password protect or secure the PDF . The maximum file size for the Report Document is 50MB.

AFOSR_Report_SCADA 05_04_15 FINAL submitted.pdf

Upload a Report Document, if any. The maximum file size for the Report Document is 50MB.

Archival Publications (published) during reporting period:

See report.

Changes in research objectives (if any):

None.

Change in AFOSR Program Manager, if any:

Former Program Manager: Dr. Robert Herklotz

Extensions granted or milestones slipped, if any:

None.

AFOSR LRIR Number

LRIR Title

Reporting Period

Laboratory Task Manager

Program Officer

Research Objectives

Technical Summary

Funding Summary by Cost Category (by FY, $K)

	Starting FY	FY+1	FY+2
Salary			
Equipment/Facilities			
Supplies			
Total			

Report Document

Report Document - Text Analysis

Report Document - Text Analysis

Appendix Documents

2. Thank You

E-mail user

Jul 07, 2015 15:17:49 Success: Email Sent to: wmahoney@unomaha.edu